
*Promoting Convenience, Choice, and Commerce on the Net*

The NetChoice Coalition
1401 K St NW, Suite 502
Washington, DC 20005
202.420.7482

www.netchoice.org

February 24, 2010

FILED ELECTRONICALLY

Before the Federal Communications Commission

In the Matter of Empowering Parents and Protecting Children
in an Evolving Media Landscape

**Comments of NetChoice—MB Docket No. 09-194**

NetChoice hereby files these comments in response to the Commission's Notice of Inquiry (NOI), MD Docket No. 09-194.

NetChoice is a coalition of the nation's leading platforms for Internet communities and e-commerce, along with several thousand small online businesses. Our members have been among the leaders in promoting safe online environments for children. Online companies have innovated in technology to empower parents and promoted legislation to educate children at an early age. At the same time, we advocate for aggressive enforcement and new regulations on child safety issues that undermine consumer trust and confidence in online information and commerce.

We welcome this opportunity to inform the Commission's NOI on empowering parents and protecting children in an evolving media landscape—realizing that the Internet is just one of many communications media on which the Commission requests information.

Social media websites have transformed the way we think about communicating. They have become a mainstream phenomenon for all ages, but particularly for children and teens. Today's kids, who were born into our digital, Internet-focused society, naturally take to social networking. Harvard professors John Palfrey and Urs Gasser call children born after 1980 "digital natives." In their book "Born Digital", the authors describe a world of issues surrounding the intensive use by digital natives of online social networks and other digital tools and media they use on a daily basis such as instant messaging, texting, video games and creating all sorts of written and video content.

The great majority of youths experience an enriching, enlightening and safe online environment. Online risks to youth—in the form of inappropriate content, advertising, or criminal predation—must be tempered with the overwhelming benefits online communities and content provide to today's youth.

**The View of Child Safety Experts: Online Risks to Child Safety Are Often Overstated**

Over the past few years, there has been an explosion of studies about the online risks to children and how sex offenders prey on children through the Internet. Initial studies focused on the new threat to children and brought attention to gaps in education and criminal statutes. Later studies have nuanced their focus and have helped identify where real risks lie and how online threats to children may differ from offline. Finally, researchers have questioned the assumption that age or identity deception is a core problem of online sexual solicitation.

The National Center for Missing and Exploited Children (NCMEC) made headlines when it first conducted its Youth Internet Safety Survey in 1999, and then followed it up with a similar survey in 2005. According to this survey, one in seven children who are regular Internet users are sexually solicited online.[1] This statistic has been quoted, cited and touted in a number of ways—but it has also been misinterpreted. With statistics, it is often necessary to "read the fine print" of the quantitative methodology.

Without context, "one in seven youths is sexually solicited online" implies large-scale predation of children by older adults. In the NCMEC study, teens were asked to report on "any situation where someone on the Internet attempted to get them to talk about sex when they did not want to or asked them unwanted sexual questions about themselves." Around 90% of the time, these solicitations were from other peers or young adults. Most solicitations involve no attempt to meet offline. Thus, the numbers do not bear out what might be considered a worst case scenario—an adult sex offender rooming or soliciting unsuspecting children.

How does these findings compare to offline circumstances? Four in five students are sexually harassed at high school, according to a 2002 study of the American Association of University Women, Hostile Hallways. Moreover, sex crimes against children are overwhelmingly committed by a friend or family member.

When offline encounters between adults and minors are initiated on the Internet, data suggests that most of the time there is no deception from the adult. The minor knows that the adult is an adult and that sex is desired. Actual cases of predation are rare.

The typical scenario for how children become victimized in the offline world by someone they first met in over the Internet is revealed best in a seminal 2004 study by the New Hampshire Crimes against Children Research Center.[2] The research documents 2,500 cases where juveniles were victims of sex crimes by people they met through the Internet. Those children—almost all of whom were teenagers—were not the victims of the classic scenario everyone fears: "strangers who are pedophiles lure a child into situations where they can be abducted or assaulted." In fact, the opposite was the case:

- Offenders did not generally deceive victims about their age and interest in sexual relationships. Only 5% of offenders lied about their age to pose as a minor.
- 80% of offenders revealed their sexual desires to the minor.
- In 89% of cases, victims willingly engaged in sexual activity with the offender. Only 5% of the cases involved physical violence or rape.

---

[1] Janis Wolak, Kimberly J. Mitchell, and David Finkelhor. *Online Victimization of Youth: Five Years Later*. Alexandria, Virginia. National Center for Missing & Exploited Children, 2006, page 1.

[2] Wolak, J., Finkelhor, D. and Mitchell, K.J. (2004). Internet-initiated sex crimes against minors: Implications for prevention based on findings from a national study. Journal of Adolescent Health, 35(5), 424-433. (CV71), available at http://www.unh.edu/ccrc/pdf/jvq/CV71.pdf

The disturbing finding of this study is that in the overwhelming number of cases young victims *knew* that the offender was an older man with sexual intentions *before* agreeing to a face-to-face encounter. Who were these children? Not surprising that most of these children were at-risk youth who were in need of guidance, love and understanding. When parents aren't present or involved, some kids look elsewhere for acceptance—including people they meet over the Internet.

Existing research suggests that deception is not occurring in most cases involving child safety, and that therefore age and identity technologies would not be helpful in revealing adult ages to children. Of course, even while many youth voluntarily to meet and have sex with adults, it is still a serious crime that takes advantage of inexperienced and vulnerable children.

**The Online Industry Continues to Empower Parents and Protect Children**

There are a number of technological tools and website design features that have been implemented to increase child safety. The Berkman Center's Internet Safety Technical Task Force study documents an entire appendix to company submissions describing efforts to increase user safety and ensure privacy.[3]

Many websites restrict access to age appropriate content, shield younger users from older members of the community, and have partnered with law enforcement in these efforts. Examples include:

- MySpace employs a search algorithm, utilizing regularly updated terms commonly used by underage users, to seek and delete the profiles of individuals misrepresenting their age. The site has safety tips on every page, including links to blocking software.
- AOL's parental control software contains pre-set age controls for web browsing: the software offers easy to navigate and control pre-set age ranges such as Kids (12 and under), Young Teen (13-15), and Mature Teen (16-17) to automatically align Web filtering and monitoring settings to provide an age-appropriate online experience.
- A growing number of sites educate users through "teachable moments" during certain user activities.
- Many sites have functionality that allows users to control their privacy settings, and give users the ability to block other users from contacting them or seeing their profile page.

Two of the best resources for learning about the numerous technology tools that monitor, filter and block unwanted content to children include:

- Progress and Freedom Foundation, Adam Thierer, *Parental Controls and Online Child Protection*, available at http://www.pff.org/parentalcontrols/

- Harvard Berkman Center, John Palfrey et al., *Enhancing Child Safety and Online Technologies: Final Report of the Internet Safety Technical Task Force to the Multi-State Working Group on*

[3] John Palfrey et al., *Enhancing Child Safety and Online Technologies: Final Report of the Internet Safety Technical Task Force to the Multi-State Working Group on Social Networking of State Attorneys General of the United States* (2008), *See* http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/ISTTF_Final_Report-APPENDIX_E_SNS.pdf

*Social Networking of State Attorneys General of the United States* (2008), available at http://cyber.law.harvard.edu/pubrelease/isttf/

**The Pitfalls of One Technology Approach: Age Verification and Parental Consent over the Internet**

In its final report to the attorneys general in December, 2008, the Berkman Center's Internet Safety Technical Task Force failed to recommend remote age and identity verification for use by online forums and social networks.[4] The report found a range of concern with identity authentication and age verification technologies. The Berkman task force also concluded that the "authentication and verification technologies submitted present privacy and security concerns."[5]

Furthermore, in its 2007 report to Congress on COPPA, the Federal Trade Commission noted that "age verification technologies have not kept pace with other developments, and are not currently available as a substitute for other screening mechanisms."[6]

The Berkman and FTC reports shied away from endorsing age and identity authentication because there are still serious issues to be resolved. There are practical challenges involved when authenticating remotely, and there are problematic unintended consequences.

There are multiple ways to attempt to confirm age and identity. With age verification, a website will attempt to identify which of its users are adults or which of its users are children. Using identity verification, a website will attempt to authenticate whether a person claiming to be "John Doe" when registering on a website is, to a reasonable degree of certainty, "John Doe." Finally, there is parental verification, which establishes whether a person claiming to be a parent of a child is in fact the parent.

Using data from public records is only as effective as the quality and completeness of the public database. That is why verifying a child's age is next to impossible online. Currently, there are no public records of minors that allow for online methods to precisely determine a child's age. Minors do not possess documents that are recognized as providing verification of identity and age, such as a driver's license. Nor do minors have the track record to answer "out of wallet" questions that ask about monthly car loan and mortgage payments. There are significant privacy concerns when any institution, including schools, store records of children.

Age and identify verification exists today for adults, most of whom to do have the "out of wallet" questions to establish online banking accounts, purchase regulated items such as alcohol, tobacco, and lottery tickets, and access adult-only content. But there is also a physical presence required for the delivery of wine. Postal carriers will check for age identification upon delivery. When a winning lottery ticket is redeemed, there is a physical presentation that affords an opportunity for the verification of age.

As opposed to its use in regulated products, age and identity verification solutions are less effective in creating safe environments for children online. Underage users or convicted sex offenders want to subvert the verification process, whereas in the e-commerce context adults typically *want* to verify their identity correctly. Credentials can easily be traded to others, leading to a "black market" for IDs and allowing for the possibility that adults can pose as children, and vice-versa.

---

[4] *Id*. *See* http://cyber.law.harvard.edu/pubrelease/isttf/

[5] *Id.*

[6] Federal Trade Commission, *Implementing the Children's Online Privacy Protection ACT: A Report to Congress*, Feb. 2007, available at http://www.ftc.gov/reports/coppa/07COPPA_Report_to_Congress.pdf

Verifying parents also has serious concerns. There are no databases or identification measures to verify that a person whom a child designates as a parent /guardian is in fact the parent/guardian. A parental consent law might actually lead parents to have a false sense of security. Parents may believe that without their permission, there is no way their children could be online and on social networking sites, when the reality is that they are online. That's why many experts view parental consent requirements to be a parental verification pitfall.

Teens are very active users of Internet websites. To verify parental consent, parents would have to provide identifying data (most often credit card information) to a myriad of sites and services. This would require private companies to store vast amounts of parents' personal information and, by doing so, increase customers' vulnerability to security breaches and identity theft. According to the Berkman study, "there are significant potential privacy concerns and security issues given the type and amount of data aggregated and collected by the technology solutions…." Many online companies have moved away from collecting and storing this type of data for good reason.

**Online Safety Requires a Comprehensive Legislative and Public Policy Approach**

In 2008, the American Legislative Exchange Council (ALEC) and Council of State Governments (CSG) adopted model, suggested state legislation to improve online safety for children. These efforts took a holistic, comprehensive approach to safety, recognizing that a child's welfare depends on parenting, education, industry efforts, and action from law enforcement when needed. The legislation's core components include:

- **Empowers Parents & Guardians**. Internet access providers must make available to subscribers a product or service that controls a child's use of the Internet.
- **Educates Children**. The legislation provides school districts with online safety curricula for children and educational materials for parents, and requires teaching online safety in the classroom.
- **Increases Post-Conviction Controls on Convicted Sex Offenders**. The legislation sets sentencing and parole guidelines that require the state to monitor the online activities of convicted child predators. The legislation also allows judges to impose restrictions on the online activities of convicted child predators.
- **Expands Sex Offender Registry Information to Include Internet Identifiers**. For states that already maintain sex offender registries that contain physical description and location information, the legislation further requires the state to collect an offender's email addresses and usernames. It would also make the email addresses of sex offenders available to any commercial or non-profit entity, including child safety organizations, educational institutions, and online services, for the purpose of protecting children from sex offenders.
- **Helps Preserve Internet Evidence for Law Enforcement Investigations**. Online services must preserve and disclose customer communications and other evidence upon request of law enforcement officials.
- **Expands the Reach and Enforcement of Child Porn Reporting**. The legislation adds state enforcement powers and broadens the scope of online companies that must report images of child porn to the Cyber Tip Line at NCMEC (National Center for Missing & Exploited Children).

- **Creates the New Crime of Internet Sexual Exploitation of a Child**. The legislation makes it a crime to use a computer or computer network to encourage a child to engage in or to observe sexual activity while communicating online.
- **Criminalizes the Internet Luring of a Child**. The legislation makes it a crime to use a computer or computer network to make sexually suggestive statements in order to lure children into face-to-face meetings.
- **Criminalizes Age Misrepresentation with Intent to Solicit a Child**. The legislation makes it a crime to lie about your age when enticing a child into criminal sexual conduct.

There are a number of states that have implemented sections of the comprehensive legislation, including Georgia, Indiana, and Louisiana. Indeed, Georgia's statute requires online education in the schools beginning in third grade. It is the impetus for Cobb County being the first school district in the nation to distribute the FTC's new publication on Internet safety, *Net Cetera: Chatting With Kids About Being Online*. [7]

**Conclusion—Online Companies Continue to Work Together with Federal and State Policymakers**

Improving child safety is a continuous exercise, and another working group will meet throughout this year to evaluate Internet safety. This latest effort is an outgrowth of the "Broadband Data Improvement Act", Pub. L. No.110–385. Section 214 of that Act directs Protecting Children in the 21st Century Act, which was signed into law by President Bush in 2008.

The law instructed the Department of Commerce's National Telecommunications and Information Administration (NTIA) to create a working group. The law specifically directed the Online Safety and Technology Working Group (OSTWG) to "review and evaluate the status of industry efforts to promote online safety through educational efforts, parental control technology, blocking and filtering software, age-appropriate labels for content or other technologies or initiatives designed to promote a safe online environment for children." The first meeting of the task force was in June 2009, and it will conclude with a report to Congress this year. NetChoice is a member of this task force.

While NTIA and FTC are active in promoting online safety, we believe that the FCC lacks jurisdiction to regulate online media platforms. Neither the Telecommunications Act of 1996 nor the Children's Television Act of 1990 provides the Commission with the authority to regulate online media content. Furthermore, if the FCC were to pursue regulation of the Internet in the same manner it regulates broadcast and cable television, we believe there would be serious first amendment implications.

[7] *See* http://www.onguardonline.gov/topics/net-cetera.aspxb

The lack of FCC jurisdiction notwithstanding, online safety is an important and evolving issue. NetChoice and our members will continue to work with state and federal policymakers and law enforcement agencies to better protect children online.

Respectfully submitted,

Braden Cox
Policy Counsel
NetChoice
1401 K St NW, Suite 502
Washington, DC 20005
(202) 420-7485